Cybercrime: xDedic illegal online marketplace dismantled

23 November 2018

On 24 January, members of the National Police and the Prosecutor General's Office of Ukraine, with assistance from members of the Federal Computer Crime Unit (FCCU) of Belgium, Europol, and the US Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) of Tampa, Florida, conducted house searches in nine places in Ukraine. Several IT systems were confiscated and three Ukrainian suspects were questioned.

The house searches were related to two criminal investigations into the xDedic Marketplace, on which access to tens of thousands of compromised servers of unknowing victims (companies and private individuals) was offered for sale. The hacking was accomplished via the Remote Desktop Protocol (RDP). Buyers and sellers traded such RDP servers on this platform for amounts ranging from USD 6 to more than USD 10 000 each.

In the first investigation, the investigating judge in Mechelen, at the request of the Belgian Federal Prosecutor's Office and the General Prosecutor's Office of Ukraine, conducted a criminal investigation. At the beginning of 2018, a JIT agreement was signed between Belgium, Ukraine, Eurojust and Europol, which was renewed early this year.

The JIT was funded by Eurojust. The investigation focused on a number of vendors on the xDedic Marketplace, who sold a large number of Belgian hacked computer systems, and the organised criminal group (OCG) that organised and operated the illegal online marketplace.

The US investigation into the OCG behind the xDedic marketplace was led by the United States Attorney's Office for the Middle District of Florida.

On 24 January, the xDedic Marketplace was made inaccessible on the orders of a US court, and the criminal IT infrastructure was confiscated. Customers who attempt to access the xDedic domain will be referred to a US government page explaining that the marketplace was taken offline. For this confiscation and inaccessibility, assistance was provided by police forces in Germany.

The Belgian Federal Prosecutor's Office started the investigation into the xDedic Marketplace in June 2016. Using special investigative techniques, the criminal infrastructure behind xDedic was made visible and digital copies of the most important criminal servers were obtained.

A thorough analysis of the content of the servers, supported by Europol and the Ukrainian National Cyber Police, led to the identification of website administrators in Ukraine. Throughout this investigation, Belgian and Ukrainian law enforcement closely coordinated their investigative efforts.

As soon as the Belgian and American criminal investigators discovered that they had shared common targets and goals, they worked together closely. In the course of 2018, Eurojust held two two-day coordination meetings, with Belgium, the USA, Ukraine and Europol, to plan the actions, provide support for the issuing and execution of the European Investigation Orders, and deal with any judicial obstacles.

Through their coordinated efforts, Belgian, Ukrainian and American judicial, prosecutorial and police authorities struck a devastating blow against the online marketplace for the illegal trade of hacked computer systems. An important signal was also sent to the perpetrators of other online criminal activities, including on the darkweb, that they are not immune from criminal investigation and prosecution. The approach to the xDedic marketplace demonstrates the importance of intensive international cooperation in the fight against organised crime on the dark web.